IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF SOUTH CAROLINA
COLUMBIA DIVISION

In The Matter of the Seizure of Funds, Monies, and Other Things of Value not to Exceed $8,204 Stored in or Accessible at Binance Account Associated with the Following "**Target Cryptocurrency Account**:" **Salaman SHAHZADA**	Case No. 3:24-cr-00182

Affidavit in Support of An Application for a Seizure Warrant

I, Clinton Walker, being first duly sworn, hereby depose and state as follows:

Introduction and Background

1. I am a Special Agent of the South Carolina Law Enforcement Division (SLED) and Task Force Officer of the United States Secret Service South Carolina Cyber Fraud Task Force (USSS SC CFTF) and have been so employed since January 2023. As a Special Agent of SLED, I received extensive training at the South Carolina Criminal Justice Academy. This training covered aspects of criminal investigation and law enforcement. I have participated in numerous investigations of violations of criminal law including matters involving fraud and white-collar crime. I have attended numerous training courses involving financial related crimes and crimes involving cryptocurrency.

2. This affidavit does not purport to set forth all my knowledge or investigation concerning this case. The statements contained in this affidavit are based on my personal knowledge or from information that I have learned during my investigation, including information from financial institutions, witnesses, and others participating in the investigation.

Requested Seizure and Target Offenses

3. I am submitting this affidavit in support of an application for a warrant authorizing agents of the USSS to seize up to the value of $8,204 in U.S. dollars from the below described wallet, hereinafter the "**Target Cryptocurrency Account:**"

> Monies, funds, and things of value at Cryptocurrency Exchange Binance, not to exceed $8,204 held in the Binance account associated with the owner:
> **Salaman SHAHZADA**

4. I respectfully submit there is probable cause to believe that the funds in the **Target Cryptocurrency Account** are unlawful proceeds of violations relating to 18 U.S.C. § 1343 (**wire fraud**) and are thereby subject to civil and criminal forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C), made applicable to criminal forfeiture by 28 U.S.C. § 2461(c). The funds described herein are also thereby subject to civil and criminal seizure pursuant to 18 U.S.C. § 981(b) and 21 U.S.C. § 853(e) and (f) by 18 U.S.C. § 982(b)(1).

Background on Cryptocurrency and Binance Exchange

5. Based on my training, research, education, and experience, I am familiar with the following relevant terms and definitions as they relate to cryptocurrency:

a. **Cryptocurrency**: Cryptocurrency, a type of virtual currency, is a decentralized, peer-to-peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency[1] or other cryptocurrencies. Examples of cryptocurrency are Bitcoin (BTC),

[1] Fiat currency is currency issued and regulated by a government such as the U.S. dollar, euro, or Japanese yen.

Litecoin (LTC), Ethereum (ETH) and Tether (USDT). Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys (described below) used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a "blockchain," which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.[2] Cryptocurrency is not illegal in the United States.

b. **Wallet**: Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public key or address is akin to a bank account number, and a private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key. To conduct transactions on a blockchain, an individual must use the public address (or "public key") and the private address (or "private key"). A public address is represented as a case-sensitive string of letters and

[2] Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

numbers, 26–36 characters long, and is somewhat analogous to a bank account number. Each public address is controlled and/or accessed through the use of a unique corresponding private key—the cryptographic equivalent of a password or PIN—needed to access the address. Only the holder of an address' private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

c. **Cryptocurrency Wallet Services**: Some companies offer cryptocurrency wallet services which allow users to download a digital wallet application onto their smart phone or other digital device. A user typically accesses the wallet application by inputting a user-generated PIN code or password. Users can store, receive, and transfer cryptocurrencies via the application; however, many of these companies do not store or otherwise have access to their users' funds or the private keys that are necessary to access users' wallet applications. Rather, the private keys are stored on the device on which the wallet application is installed (or any digital or physical backup private key that the user creates). As a result, these companies generally cannot assist in seizing or otherwise restraining their users' cryptocurrency. Nevertheless, law enforcement could seize cryptocurrency from the user's wallet directly, such as by accessing the user's smart phone, accessing the wallet application, and transferring the cryptocurrency therein to a law enforcement-controlled wallet. Alternatively, where law enforcement has obtained the recovery seed for a wallet (see above), law enforcement may be able to use the recovery seed phrase to recover or reconstitute the wallet on a different digital device and subsequently transfer cryptocurrencies held within the new wallet to a law

enforcement-controlled wallet.

d. **Use of Cryptocurrency in Criminal Activity**: Although cryptocurrencies such as Bitcoin, Ethereum and Tether have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes such as money laundering and is often used as payment for illegal goods and services. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track transactions.

e. **BTC Value in U.S. Dollars**: As of January 10, 2024, one BTC is worth approximately $45,703, though the value of BTC is generally much more volatile than that of fiat currencies.

f. **Exchanges:** Cryptocurrency "exchangers" and "exchanges" are individuals or companies that exchange bitcoin for other currencies and cryptocurrencies, including U.S. dollars and Tether/USDT. Exchanges can be brick-and-mortar businesses or online businesses (exchanging electronically transferred money and virtual currencies). According to Department of Treasury, Financial Crimes Enforcement Network ("FinCEN") guidance issued on March 18, 2013, virtual currency administrators and exchangers, including an individual exchanger operating as a business, are considered money services businesses.[3] Such exchanges and exchangers are required to register with FinCEN and have proper state licenses (if required under applicable state law). Based on my training and

[3] *See* "Application of FinCEN's Regulations to Person Administering, Exchanging, or Using Virtual Currencies," *available at* https://www.fincen.gov/resources/statutes-regulations/guiadance/application-fincens-regulations-persons-administering.

experience, I know that registered money transmitters are required by law to follow Bank Secrecy Act anti-money laundering ("AML") regulations, "Know Your Customer" ("KYC") protocols, and other verification procedures similar to those employed by traditional financial institutions. For example, FinCEN-registered cryptocurrency exchangers often require customers who want to open or maintain accounts on their exchange to provide their name, address, phone number, and the full bank account and routing numbers that the customer links to an exchange account. As a result, there is significant market demand for illicit cryptocurrency-for-fiat currency exchangers, who lack AML or KYC protocols and often also advertise their ability to offer customers stealth and anonymity. These illicit exchangers routinely exchange fiat currency for cryptocurrencies by meeting customers in person or by shipping cash through the mail. Due to the illicit nature of these transactions and their customers' desire for anonymity, such exchangers are frequently able to charge a higher exchange fee, often as high as 9–10% (in contrast to registered and BSA-compliant exchangers, who may charge fees as low as 1–2%).

g. **Exchange Transactions**: Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible, external device ("hardware wallet"), downloaded on a PC or laptop ("desktop wallet"), with an Internet-based cloud storage provider ("online wallet"), as a mobile application on a smartphone or tablet ("mobile wallet"), printed public and private keys ("paper wallet"), and as an online account associated with a cryptocurrency exchange. Because these desktop,

mobile, and online wallets are electronic in nature, they are located on mobile devices (e.g., smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the Internet. Moreover, hardware wallets are located on some type of external or removable media device, such as a USB thumb drive or other commercially available device designed to store cryptocurrency (e.g. Trezor, Keepkey, or Nano Ledger). In addition, paper wallets contain an address and a QR code[4] with the public and private key embedded in the code. Paper wallet keys are not stored digitally. Wallets can also be backed up into, for example, paper printouts, USB drives, or CDs, and accessed through a "recovery seed" (random words strung together in a phrase) or a complex password. Additional security safeguards for cryptocurrency wallets can include two-factor authorization (such as a password and a phrase). I also know that individuals possessing cryptocurrencies often have safeguards in place to ensure that their cryptocurrencies become further secured in the event that their assets become potentially vulnerable to seizure and/or unauthorized transfer.

h. **Binance**: Binance is a global cryptocurrency spot and derivatives exchange. They report to be the larger cryptocurrency in terms of daily volume. Binance serves customers from around the world but does not do business in the United States. There is no official company headquarters, but the organization was founded in 2017 in Shanghai, China.

[4] A QR code is a matrix barcode that is a machine-readable optical label.

Probable Cause

Use of Target Cryptocurrency Wallet in Wire Fraud

6. On 12/19/23 SLED Investigators were contacted by a compliance specialist of Carolina's Telco Federal Credit Union (CTFCU) in reference to a customer that was the victim of a fraud involving Bitcoin. I responded to the CTFCU office located at 110 Outlet Point Blvd, Columbia, S.C. 29210 and met with the reporting party as well as employees of CTFCU. The following description was relayed to me as well as a written statement provided by the reporting party (*Appendix* A). Based on the information obtained during the investigation, a scheme to defraud the victim occurred between the dates of 12/18/23 and 12/19/23 in violation of 18 U.S.C. § 1343 (**wire fraud**) by an unidentified group of subject(s) with the direct involvement and facilitation of **Salaman SHAHZADA.**

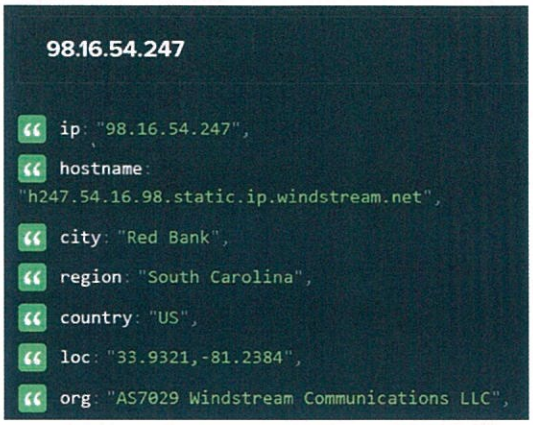
7. The reporting victim was transferred between several individuals during the course of the fraudulent scheme. Several subjects provided names and phone numbers while purporting to be affiliated with Etsy.com. All subjects were working in concert to defraud the victim and commit the violation of 18 U.S.C. § 1343 (**wire fraud**). The subjects provided the following names and positions to the victim:

Steve Lambert (Account Manager)	1-786-342-1282
Frank (Senior Employee)	1-310-742-4573
Alex Smith (Employee)	1-786-233-1530

For the purposes of this probable cause statement, the subjects will be known as Fraud-ring Members (FM).

8. On 12/18/2023 Victim 1 attempted to call the customer service line of www.Etsy.com (online retailer of craft goods) to inquire about a refund. Victim 1 placed the call from Lexington, S.C. Victim 1 stated his wife paid $213.00 on the e-commerce site for a custom painting two months prior to placing the call. The items purchased were not received. Victim 1 was connected with an individual FM.

9. FM instructed Victim 1 to use his personnel computer to start the refund process. Victim 1 proceeded to use his personal computer, HP Laptop Model:17-BU4061NR, for the supposed refund activity. Victim 1 relayed to me he is not very familiar with computers and did not conduct banking transactions online. Prior to 12/18/23, Victim 1 stated that he did not have online banking enabled with CTFCU. Based on information provided from Victim 1 and representatives of CTFCU, it is my belief that FM(s) connected to Victim 1's computer through a remote desktop application and created an online banking profile with CTFCU. The remote desktop application enabled FM(s) to make it appear as if Victim 1 was activating the online banking functionality for his accounts. Victim 1 provided FM with the requisite banking information that would allow FM to enroll Victim 1 in online banking through CTFCU. The IP address that was used to create the profile as reported by CTFCU was "**98.16.54.247**". Based on open-source searches, the Internet Protocol address (IP) is registered to Windstream Communications LLC, Victim 1's internet service provider, and is allocated to an address in the Lexington area consistent with Victim 1's address.



Opensource information detailing the owner and location assigned to the IP used in the fraud.

10. Victim 1 subsequently submitted the laptop for repair due to the fraudulent activity. A receipt from the repair location indicated 3 instances of unidentified malware located on the machine. *(See Appendix A)*.

11. With access to Victim 1's computer and banking account, FM conducted a credit card cash advance of $10,000 from the victim's account. FM told Victim 1 an error was made during the refund process. FM stated $10,000 was refunded to Victim 1 and money was transferred to Victim 1's account in error. Victim 1 confirmed, through a call to CTFCU's automated over-the-phone-balance number, that $10,000 had been transferred into the account. The source of the money was the $10,000 credit card cash advance that FM made against Victim 1's credit card and transferred to Victim 1's account. I know based on my training and experience this is a common tactic used by fraud subjects. This tactic makes the account appear as though a transfer of outside funds has occurred.

0000210607 S 0015	12/18/2023	12/18/2023	Deposit	Online banking	Transfer	Credit Card Cash Advance: Transfer from L 5101	10,000.00	13,009.09

Victim 1 banking transactions provided by CTFCU. Transaction on 12/18/2023 depicting a Credit Card Cash Advance 0f $10,000 to the victim's CTFCU checking account. See Appendix A.

12. FM instructed Victim 1 to withdraw $9,787 from his checking account and send the money to back to the FM. FM stated the transfer must be completed quickly and indicated to Victim 1 that FM's job was in jeopardy if the funds were not returned. Based on training and experience, I know this is a common tactic used to illicit finds from victims of fraud.

13. FM directed Victim 1 to lie to the bank employee if asked about the use of the withdrawn funds. Victim 1 was instructed by the unknown subjects to tell bank employees that the funds were being used to purchase Christmas gifts or to pay for grounds keeping work. Victim 1 withdrew the funds from his account at CTFCU. *(See Appendix A for receipt).*

14. Victim 1 was then directed to the BTMMachines cryptocurrency ATM located at 1601 Broad River Rd, Columbia, S.C. 29210. The ATM is located inside the Halal International market located at the same address. I spoke to employees of Halal International market who recalled an individual matching Victim 1's description using the BTMMachines ATM for approximately 45 minutes.

15. Victim 1 was sent a bitcoin address in multiple forms from FM using multiple phone numbers and directed to place the $9,787 withdrawn from the victim's account into the cryptocurrency ATM. The victim received a QR code and subsequent bitcoin address identified as 'bc1qjw288xq6x4p7gfuzxu5w8xgka6rk93qm2u68lq'.

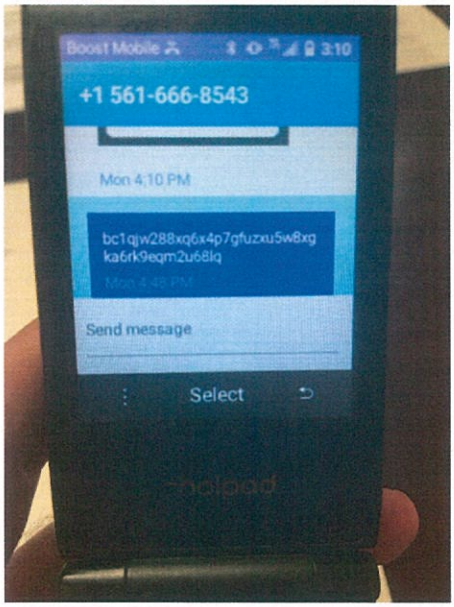


Image of Victim 1's phone displaying the bitcoin address sent by phone number +1 561-666-8543.

16. Victim 1 used the BTMMachines built-in scanner to scan the sent QR code when prompted. Employees of BTMMachines contacted the victim and allowed the transaction to continue. Victim 1 completed the transaction and discontinued communication with FM(s).

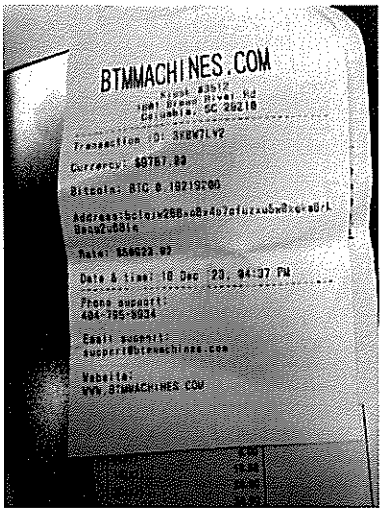
17. On 12/19/23 Victim 1 received a follow up call from FM(s) and was told that an additional transaction had been conducted and the victim would need to send another $11,000. Victim 1 then traveled to the CTFCU branch located at 110 Outlet Point Blvd, Columbia, S.C. 29210. After speaking with an employee of CTFCU, Victim 1 learned he had been the victim of a fraud scheme.

18. I was alerted to the fraud and responded to the CTFCU location. I made contact with Victim 1 and gathered evidence related to the fraud. FM(s) contacted Victim 1 and requested he travel to the BTMMachines cryptocurrency ATM while in my presence using multiple numbers. Victim 1 was advised to discontinue contact with FM(s) and employees of CTFCU worked to

secure Victim 1's bank accounts.

Cryptocurrency Transactions

19. Victim 1 presented me with a BTMMachines.com receipt dated 12/18/24 04:37 PM for the amount of 0.19219206 BTC (Approx. $8,204 USD). I called and spoke with representatives of BTMMachines.com who confirmed the transaction took place on their machine and stated they do not have a fee refund policy available to victims of frauds. BTMMachines representative stated that all AML procedures were followed pursuant to the company's policies and procedures.



Picture of BTMMachines.com transaction receipt provided by Victim 1.

20. Law enforcement can use commercially available software to trace cryptocurrency from the inception of the funds to the ultimate destination account. I have received specific training and is certified by the company in the use of the cryptocurrency tracing software. I used tracing software on this transaction. (*See Appendix B*). This tracing report shows a portion of the funds that were deposited by Victim 1 on December 18, 2023 were ultimately transferred to the **Target Cryptocurrency Account.**

21. Of the original 0.19219206 BTC sent by the victim, 0.173913 BTC was deposited

into BTC Wallet '*1EJm5ZDX63fjNx6cGKCpqVYoRN2nbVxmA9*' (**Target Cryptocurrency Wallet**) on 12/19/23 at 17:35 EST. Using commercially available software, I determined that the **Target Cryptocurrency Wallet** is associated with **Binance**. I then sent a legal request for ownership information to Binance. Binance returned the ownership and transaction information during the timeframe of the fraud. The owner of the wallet is **Salaman SHAHZADA** (DOB: 1/3/92) of 107 K Kajiyan, Muzaffarnafar, Uttar Pradesh, India. Transactions dating back to 5/27/21 in the **Target Cryptocurrency Wallet** have been assigned to **SHAHZADA.** The deposit history provided by Binance matches the information found in the cryptocurrency trace. The **Target Cryptocurrency Wallet** at the time of the request was 0.17391943 BTC and a deposit matching the information was found during the cryptocurrency tracing.

BTC	Bitcoin	0.17391943

***Target Cryptocurrency Wallet** account balance.*

Currency	Amount	USDT	Deposit Address	Source Address	Create Time
BTC	0.17391304	7594.59637	1EJm5ZDX63fjNx6cGKCpqVYoRN2nbVxmA9	bc1qjw288xq6x4p7gfuzxu5w8xgka6rk9eqm2u68lq	2023-12-20 00:16:32

***Target Cryptocurrency Wallet** deposit history (Note UTC time).*

KYC information provided by Binance.

22. IP address logs provided by Binance are consistent with an individual located in India logging into and out of the **Target Cryptocurrency Account.**

23. I inspected the information returned from Binance and determined that there was a high likelihood of additional fraudulent activity associated with the **Target Cryptocurrency Account.** I then conducted law enforcement database searches and discovered two additional reports of fraudulent payments being sent to the **Target Cryptocurrency Account.** Both reports were submitted during the period in which **SHAHZADA** had control over the account.

24. Based on the information gathered during the investigation, I requested a temporary freeze be placed on the **Target Cryptocurrency Wallet.** This request was honored by Binance and the identified fraudulently obtained funds (0.173913 BTC, Approx. $7,370 USD) were transferred into a Binance controlled account.

25. As for the funds I am seeking authority to seize, I am respectfully seeking authority to seize funds in the **Target Cryptocurrency Account** in an amount not to exceed the value of

$8,204 in U.S. dollars. That value represents the proceeds obtained from the fraud scheme perpetrated on Victim 1. (*See Appendix B*).

Conclusion and Authority

26. Though the **Target Cryptocurrency Wallet** is believed to be located outside the District of South Carolina, 18 U.S.C. § 981(b)(3), as amended by the Civil Asset Forfeiture Act of 2000 ("CAFRA"), Pub. L. No. 106-185, 114 Stat. 202 (2000), provides jurisdiction for the issuance of seizure warrants for property located in other districts. That is, the issuance of the seizure warrant in this district is appropriate under 18 U.S.C. § 981(b)(3), and 28 U.S.C. § 1355(b)(1) because, notwithstanding the provisions of Rule 41(a) of the Federal Rules of Criminal Procedure, a seizure warrant may be issued by a judicial officer in any district in which a forfeiture action against the property may be filed.

27. Thus, the issuance of the seizure warrant in this district is appropriate under the above statute, as this is the district "in which … the acts or omissions giving rise to the forfeiture occurred," and based on my training and experience, this is a continuance of an "investment scam" that began with the original victim who is based in Columbia, S.C. Further, "venue for the forfeiture action . . . is specifically provided for in section 1395." 28 U.S.C. § 1355(b)(1)(A) and (B). Section 1395 provides "for the recovery of a . . . forfeiture . . . in the district where it accrues."

28. I submit there is probable cause to believe the funds in the Target Cryptocurrency Wallet are proceeds traceable to violations of 18 U.S.C. § 1343 (wire fraud) and subject to civil and criminal forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(C) made applicable to criminal forfeiture by 28 U.S.C. § 2461(c); and are thereby also subject to seizure pursuant to 18 U.S.C. § 981(b) and 21 U.S.C. § 853(e) and (f) by 18 U.S.C. § 982(b)(1).

29. Further, a restraining order would not be adequate to preserve the property for forfeiture as the funds in the cryptocurrency account can be easily moved, transferred, or dissipated. Therefore, I respectfully request the issuance of a seizure warrant that will authorize the seizure of funds contained in the cryptocurrency account described herein.

This affidavit has been reviewed by Assistant U.S. Attorney Carrie Fisher Sherard.

[signature page to follow]

I swear, under penalty of perjury, that the foregoing is true and correct to the best of my knowledge.

Clinton Walker
Task Force Officer
United States Secret Service Cyber Fraud Task Force

SWORN TO ME VIA TELEPHONE OR
OTHER RELIABLE ELECTRONIC MEANS
AND SIGNED BY ME PURSUANT TO
FED. R. CRIM. P. 4.1 AND 4(d) OR 41(d)(3),
AS APPLICABLE

This 17th day of January 2024
Columbia, South Carolina

THE HONORABLE PAIGE J. GOSSETT
UNITED STATES MAGISTRATE JUDGE